UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,793	08/04/2006	Paul C. Kocher	2007014 / CRYP3CIP1US	3031

73091 7590 10/28/2008

Marc P. Schuyler
P.O. Box 2535
Saratoga, CA 95070

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/563,793	KOCHER ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 11-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 11-19* is/are rejected.

7)☒ Claim(s) *5-7 and 12-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/4/2008, 6/22/2007, 10/10/2006, 2/17/2006, 1/6/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the filing of June 18, 2008. Claims (1-7 and 11-19) are pending and have considered below.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1 recites the limitation "said storage" in line 7. There is insufficient antecedent basis for this limitation in the claim. Applicant is advised to review claims as presented with careful consideration of antecedent basis because there are a substantial number of antecedent basis issues within presented claims. Additional antecedent basis rejection for record:

a. Claim 1 recites the limitation "said instruction" in line 16. There is insufficient antecedent basis for this limitation in the claim.

b. Claim 5 recites the limitation "said executing device " in line 9. There is insufficient antecedent basis for this limitation in the claim.

c. Claim 6 recites the limitation "said executing device" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Due to the substantial number of antecedent basis issues existing in present claims Examiner respectfully advises applicant to carefully review claims and make appropriate correction.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the ejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4 Claims 1-7 and 11-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Traw et al. (US Patent No. 6,542,610 and Traw hereinafter).

5. As to claim 1, Traw teaches a **method for regulating access to nonvolatile digital storage contained in a device executing instructions in a Turing-complete interpreter, said method comprising:**

(a) **receiving a request from said instructions being executed** (i.e., … teaches n accordance with the present invention, a compliant device ("Device A") which is a source of protected content (e.g., a DVD player) is requested to transmit protected content across a serial bus to another compliant device ("Device B") which is a sink for protected content (e.g., a PC running an MPEG-2 video stream decoder) [col. 6, lines 40-46]), **where said request specifies** : (i) **a portion of said storage for which**

access is requested (i.e., … teaches a request to transmit protected content [col. 6, lines 45-50]), and (ii) **a plurality of additional executable instructions** (i.e., ... teaches preliminary authentication must be initiated if authentication has not been setup [col. 6, lines 50-60]);

(b) **applying a cryptographic hash function to said additional executable instructions to obtain a hash value** (i.e., … teaches applying cryptographic hash resulting a hash function may be applied to a paired 54-bit content key [col. 7, lines 30-35]);

(c) **authenticating said hash value** (i.e., … teaches both devices verifies appropriate response to challenge [col. 7, lines 5-10]);

and (d) **provided that said authentication is successful, enabling access by said instructions being executed to said requested portion of said storage while executing said additional executable instructions** (i.e., ... teaches if response is successful a channel key between Device A and Device B is generated for which provides access to the protected content [col. 7, lines 45-55]).

6. As to claim 2, Traw teaches a **method where said step of authenticating comprises comparing said hash value with a hash value stored in said nonvolatile storage** (i.e., ... teaches comparing hash data to determine if matches expected value [col. 16, lines 30-40])).

7. As to claim 3, Traw teaches a **method where said step of authenticating comprises verifying a digital signature provided by said instructions being executed** (i.e., .. teaches verifying message signature [408, fig. 4(a)]).

8. As to claim 4, Traw teaches a **method where said request includes a pointer to said additional executable instructions in memory accessible by said instructions being executed and contained in said device (**fig. 4(a)).

9. As to claim 5, Traw teaches a **digital optical disc medium containing encrypted audiovisual content for playback on any of a plurality of device architectures** [col. 12, lines 40-45]**, said digital optical disc medium comprising program logic configured to:**

(a) identify at least one characteristic of a device executing said program logic (i.e., … teaches a each device identifies a challenge value associated with the other device [col. 8, lines 30-40] … teaches identify correct message signature (i.e., characteristic) between devices [col. 8, lines 40-50]);

(b) **use said at least one characteristic** (i.e., challenge value) **to determine which, if any, of a plurality of security weaknesses are present in said executing device** (i.e., ... teaches compares challenge value of device A with challenge value of device B. ... teaches authentication is based on equivalent challenge values [col. 7, lines 36-41] … further teaches authentication of message signatures [col. 8, lines 55-60]);

(c) **when said determination indicates a suspected weakness** (i.e., … teaches determining the signature is invalid, deeming a security treat [col. 8, lines 40-55]), (i) **select at least one of a plurality of software countermeasures** (e.g., do not send protected content), **wherein said selected countermeasure corresponds to said suspected weakness and is compatible with said executing device** [col. 8, lines 40-55]; (ii) **mitigate said suspected weakness by directing said executing device to invoke said selected countermeasure** (e.g., do not send protected content) (i.e., … teaches if signature is not valid do not send protected content [col. 8, lines 50-60]); and (iii) **decode said encrypted audiovisual content** (i.e., .. teaches standard implementations of Blowfish, the permutation and substitution functions are derived from the hexadecimal digits of .pi. and the specific key being used to encrypt/decrypt data within the content protection system. [col. 5, lines 10-25]). … teaches in this content protection system, Blowfish can be modified to allow the use of alternate initialization values for the permutation and substitution functions for decrypting data [col. 5, lines 10-25]), **wherein said decoding includes a result produced by successful operation of said countermeasure logic** [fig. 7];

and (d) **when said determination does not indicate a suspected weakness, decode said audiovisual content using at least one decryption key derived using at least one cryptographic key associated with said executing device** [fig. 6 and fig. 7].

10. As to claim 6, Traw teaches a **digital optical disc medium where said program logic is configured to execute in an interpreter common to said plurality of device architectures** [fig. 8], **and at least a portion of said selected countermeasure** (i.e., embodiment) **is configured to be executed directly as native code on a microprocessor associated with said executing device** (i.e., … teaches embodiments of the present invention may be implemented in hardware, or software executed by a computing device such as a microcontroller or microprocessor [col. 5, lines 45-50]).

11. As to claim 7, Traw teaches a **digital optical disc medium where said digital optical disc medium further includes a digital signature authenticating said native code portion** (i.e., … teaches validating message signature using DSA technology [col. 5, lines 50-60; 408,fig. 4(a)]).

12. As to claim 11, Traw teaches a **automated method for determining whether to allow a portion of software stored in a computer-readable memory to access a portion of a nonvolatile memory, the method comprising:**

(a) **receiving a reference** (i.e., request for protected content) **to said portion of software** (i.e., … teaches n accordance with the present invention, a compliant device ("Device A") which is a source of protected content (e.g., a DVD player) is requested to transmit protected content across a serial bus to another compliant device ("Device B")

which is a sink for protected content (e.g., a PC running an MPEG-2 video stream decoder) [col. 6, lines 40-46]);

(b) **computing a cryptographic hash of said software portion** [col. 7, lines 30-35];

(c) **comparing said computed cryptographic hash with a value stored in said nonvolatile memory** [col. 13, lines 35-40],

(d) **when said computed cryptographic hash matches said stored value, allowing said software portion to access said nonvolatile memory portion** (i.e., $K_{pre\_control}$) [312, 316, fig. (a)};

and (e) **when said computed cryptographic hash does not match said stored value, not allowing said software portion to access said nonvolatile memory** (i.e., $K_{pre\_control}$) [312, 314, fig. (a)].

13. As to claim 12, Traw teaches a **digital optical disc where said program logic is further adapted to cryptographically authenticate at least one of manufacturer, model, and version of the device executing said program logic** (i.e., .. teaches verifying device certificate is valid. [col. 14, lines 60-67]. Those skilled in the art would recognize the device certificate [e.g.., X.509] contains version information pertinent to the device).

14. As to claim 13, Traw teaches a **digital optical disc where said program logic is adapted to verify as at least one characteristic of the device whether the device**

can perform block cipher operations using a key characteristic of at least one of manufacturer, model, and version of the device [316, fig. 3(a)].

15. As to claim 14, Traw teaches a **digital optical disc where said program logic is adapted to verify as at least one characteristic whether unauthorized firmware is present on the device** (i.e., … teaches authenticating software components running on the PC [col. 11, lines 60-67]).

16. As to claim 15, Traw teaches a **digital optical disc where said program logic is configured to access a server over a network and to receive from the server data representing at least one of code configured to identify a new characteristic, code implementing a countermeasure, revocation status, payment information associated with content, download of bonus content, and download of advertisement** (i.e., … teaches each device manufactured will have a unique device ID and public/private DSS key pair. … teaches with unique device IDs and DSS keys, the Digital Transmission Protection Authority will only need to revoke the certificates of the specific devices which have been compromised. … teaches other users who bought the same device model and have not violated the license agreement would not be effected by this revocation [col. 11, lines 50-55]).

17. As to claim 16, Traw teaches a **digital optical disc where said program logic is configured to identify a characteristic by searching a portion of memory of the device** [col. 8, lines 18-25].

18. As to claim 17, Traw teaches a **digital optical disc where said program logic is configured to identify a characteristic by accessing non-volatile storage of the device** [col. 8, lines 18-25].

19. As to claim 18, Traw teaches a **digital optical disc where said program logic is further configured to make video playable by applying modifications to a video data stream** [col. 6, lines 39-46].

20. As to claim 19, Traw teaches a **digital optical disc where said program logic is further configured to change, when applying said modifications, audiovisual content to embed forensic information** (i.e., embedded controller) **associated with playback environment** [col. 6, lines 58-62].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431